OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

HIGHLIGHTS

April 30, 2014
Cloud Computing Contract Clauses
Report Number SM-MA-14-005

BACKGROUND:

Cloud computing uses remote servers on the Internet to manage, store, and process data. Using cloud computing reduces costs while increasing the efficiency of services; however, it also has risks associated with data leaks and loss of public trust. U.S. Postal Service Supply Management (Technology Infrastructure Portfolio) contracting officials awarded 13 contracts totaling about $303 million for cloud computing services from fiscal years 2007 to 2013. The Postal Service's *Information Security* handbook of 2002 was in effect when officials awarded these contracts.

The Council of Inspectors General on Integrity and Efficiency issued a memorandum in 2011 on information accessibility, data security, and privacy concerns that federal agencies should consider before entering into cloud computing contracts. The memorandum identifies areas of concern for federal agencies but is not mandatory for the Postal Service. In August 2013, the Postal Service issued the *Cloud Security* handbook establishing information security policies and requirements to protect its information in a cloud computing environment.

Our objective was to assess whether cloud computing contracts have adequate controls to address information accessibility, data security, and privacy concerns.

WHAT THE OIG FOUND:

The 13 cloud computing contracts did not address information accessibility and data security for network access and server locations because the *Information Security* handbook in effect at the time of the contract award did not include these requirements. In addition, the Postal Service exempted a supplier from following the handbook for one contract that did not contain sensitive data. Although the data may not be sensitive, the handbook provides additional requirements such as insurance against losses resulting from data breaches and procedures for timely notification of these breaches.

The Postal Service's *Cloud Security* handbook addresses the information accessibility and data security gaps. However, contracting officials were concerned that including the policy in existing cloud computing contracts could increase contract costs. As a result, we identified potential costs of $12,429,228 for mitigating cloud security risks.

WHAT THE OIG RECOMMENDED:

We recommended management include *Information Security* and *Cloud Security* handbook requirements in future cloud computing contracts, regardless of data sensitivity, and assess the costs and benefits of incorporating these requirements into existing cloud computing contracts.